تكوين موجز إستجابة تهديد SecureX لحظر URL على FirePOWER

المحتويات

المقدمة

يوضح هذا المستند كيفية إنشاء معلومات إستخبارية حول التهديدات من عناوين URL و IPs التي تم العثور عليها أثناء التحقيقات الخاصة بالاستجابة للتهديدات التي سيتم إستهلاكها بواسطة FirePower.

معلومات أساسية

الاستجابة للتهديدات من Cisco هي أداة قوية قادرة على التحقيق في التهديدات عبر البيئة بأكملها بفضل المعلومات من وحدات متعددة. توفر كل وحدة معلومات تم إنشاؤها بواسطة منتج الأمان مثل Firepower، ونقطة النهاية الآمنة، و Umbrella، والموردين الآخرين التابعين لجهات خارجية. لا تساعد هذه التحقيقات في الكشف عما إذا كان هناك تهديد على النظام فحسب، بل تساعد أيضا في توليد معلومات مهمة حول التهديدات، والتي يمكن الحصول عليها من المنتج الأمني لتعزيز الأمن في البيئة.

بعض المصطلحات الهامة التي تستخدمها ميزة "الاستجابة لتهديد SecureX":

- **المؤشر** عبارة عن مجموعة من الملاحظات التي ترتبط منطقيا بالمشغلين و AND. وهناك مؤشرات معقدة تجمع بين نشرات متعددة، إضافة إلى أن هناك أيضا مؤشرات بسيطة مصنوعة من مؤشرات يمكن ملاحظتها فقط.
- **القالب** للملاحظة وهو متغير يمكن أن يكون IP أو مجال أو URL أو SHA256.
- يتم إنشاء **الأحكام** بواسطة المستخدم ويتم إستخدامها لربط الأحكام القالبة للملاحظة بالمصير النهائي لفترة زمنية محددة.
- يتم إنشاء **موجز ويب** لمشاركة معلومات التهديد التي تم إنشاؤها بواسطة تحقيق الاستجابة لتهديدات SecureX مع منتجات الأمان الأخرى مثل جدران الحماية وعوامل تصفية محتوى البريد الإلكتروني مثل Firepower و ESA.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- SecureX CTR (الاستجابة لتهديدات Cisco .
- TID الخاص ب Firepower (مدير معلومات التهديد).
- تكوين سياسات التحكم في الوصول إلى Firepower.

يستخدم هذا المستند FirePOWER TID لفرض المعلومات الاستخباراتية الخاصة بالتهديدات التي تم إنشاؤها حول إستجابة تهديدات SecureX. فيما يلي متطلبات إستخدام TID على نشر FMC الخاص بك إصدار 7.3 من FMC:

- الإصدار 6.2.2 وأ إصدار أحدث.
- يتم تهيئته بذاكرة سعة 15 جيجابايت كحد أدنى.
- تم التكوين مع تمكين وصول REST API. راجع تمكين وصول REST API في دليل إدارة مركز إدارة جدار الحماية الآمن من Cisco .
- يمكنك إستخدام FTD كعنصر مدير معلومات التهديد إذا كان الجهاز على الإصدار 6.2.2 وأ أعلى.

ملاحظة: تعتبر هذه الوثائق أن مدير إستخبارات التهديدات نشط بالفعل على النظام. لمزيد من المعلومات حول التكوين الأولي ل TID واستكشاف أخطاء الارتباطات وإصلاحها، راجع قسم "المعلومات ذات الصلة" المتوفرة في هذا المستند.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- لوحة التحكم في الاستجابة لتهديدات SecureX من Cisco
- FMC (مركز إدارة جدار الحماية)، الإصدار 7.3
- FTD (الاستجابة لتهديد جدار الحماية)، الإصدار 7.2

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. تبدأ جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهم للتأثير المحتمل لأي أمر.

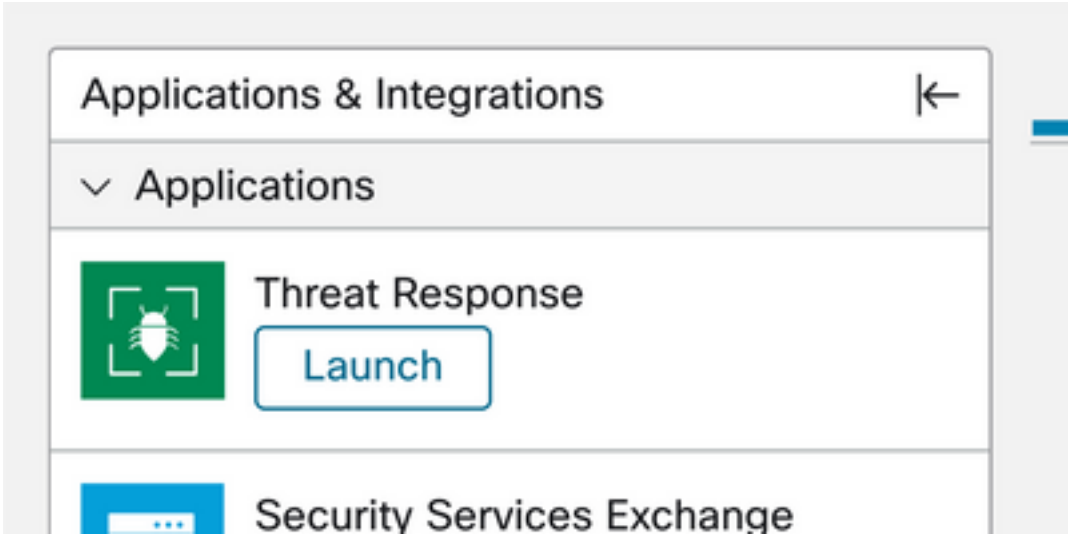
التكوين

إنشاء موجز الاستجابة لتهديدات SecureX

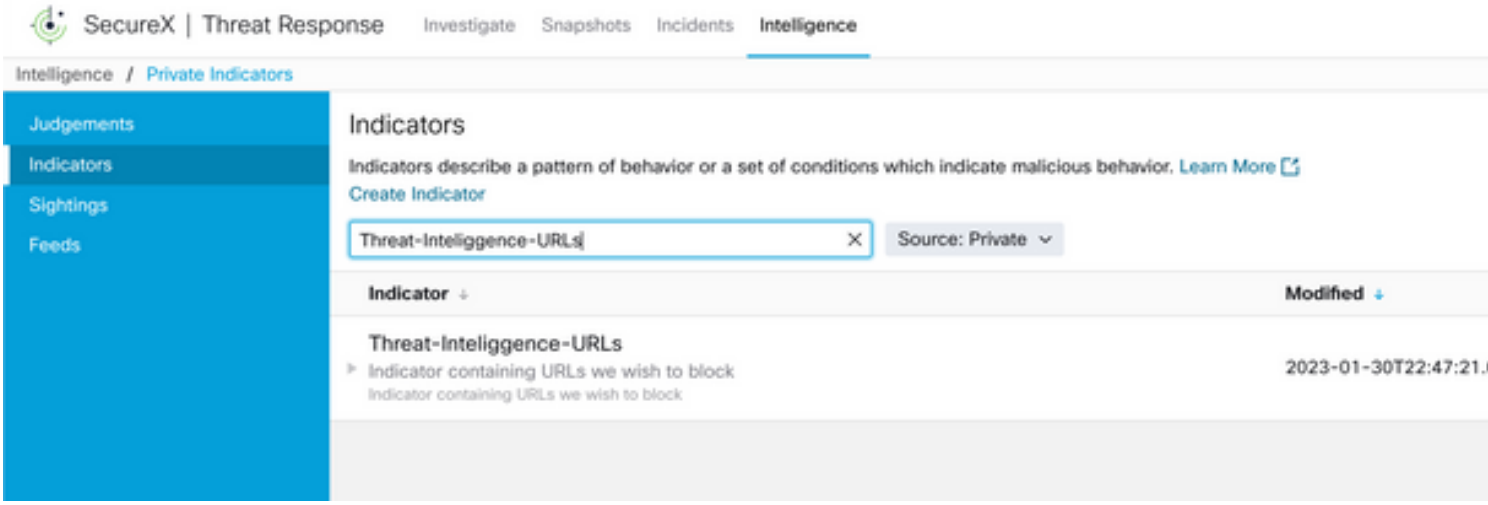
تتيح ميزة "الاستجابة لتهديدات SecureX" إمكانية بدء تحقيق في البيئة من خلال مساهمة يمكن ملاحظتها. يستعلم محرك الاستجابة للتهديدات الوحدات النمطية للبحث عن أي نشاط متعلق بالملاحظة. يقوم التحقيق بإرجاع أي تطابق تم العثور عليه بواسطة الوحدات النمطية، ويمكن أن تتضمن هذه المعلومات عناوين IP أو المجالات أو رسائل بريد URL أو الملفات. الخطوات التالية أنشئ موجز وبي لاستهلاك المعلومات مع منتجات الأمان الأخرى.

الخطوة 1 سجل الدخول إلى لوحة معلومات SecureX وانقر فوق رز **التشغيل** الوحدة النمطية ذاك "الاستجابة للتهديدات". يؤدي ذلك إلى فتح صفحة "الاستجابة للتهديدات"

جديدة:

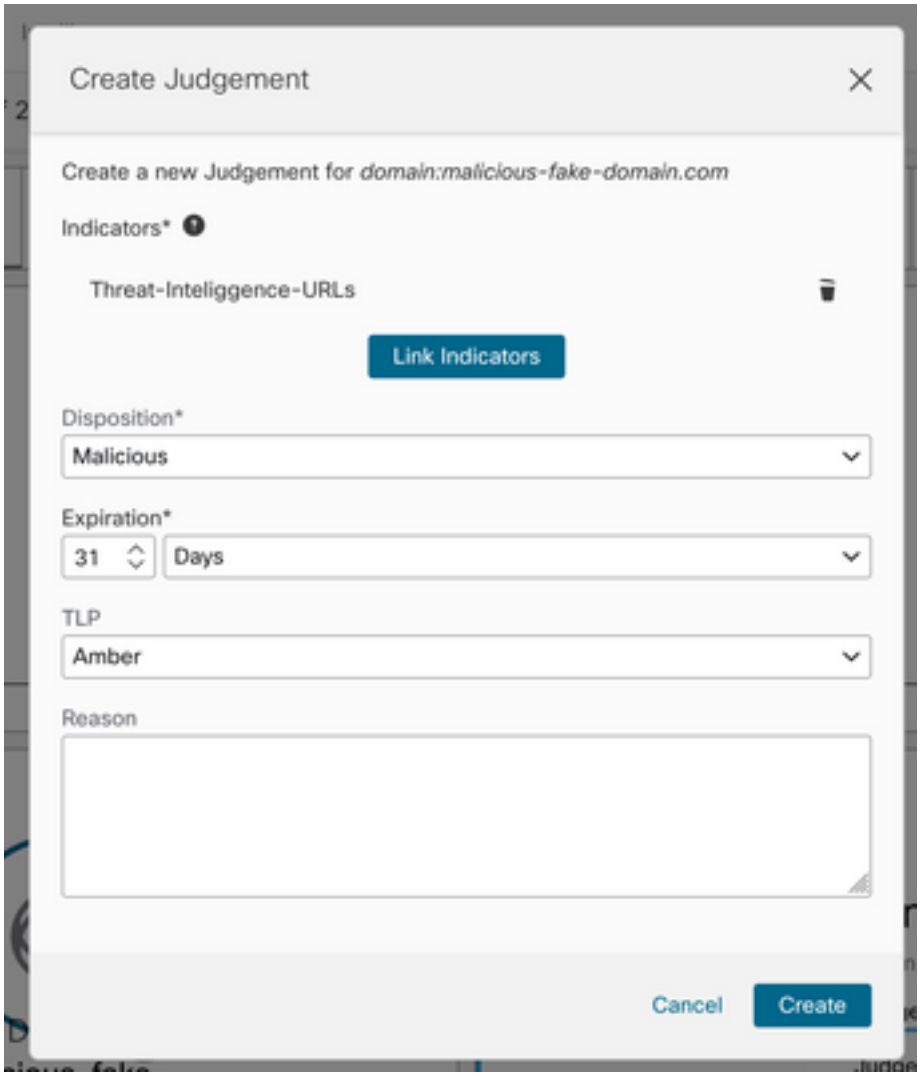


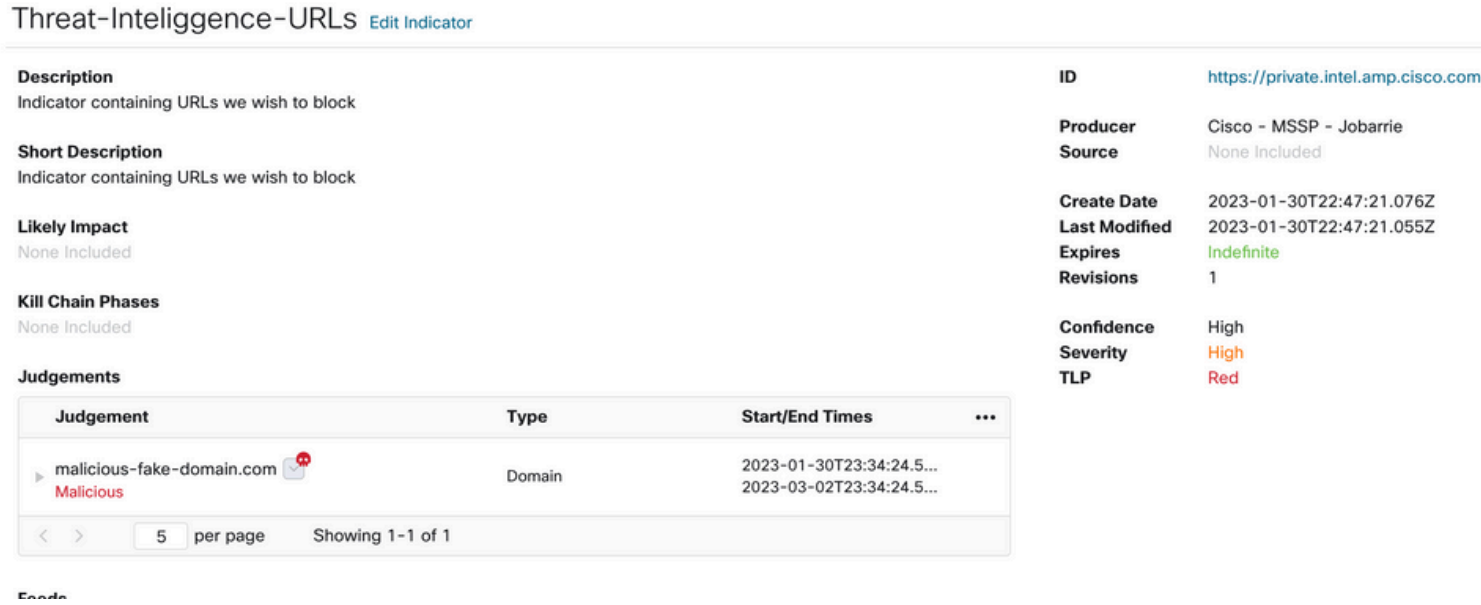
الخطوة 2 في صفحة "الاستجابة للتهديدات" انقر فوق "الذكاء" > "المؤشرات" ثم قم بتغيير القائمة المنسدلة "المصدر" من "عام" إلى "خاص". يجب أن يسمح لك ذلك بالنقر فوق إنشاء إرتباط مؤشر. بمجرد أن يدخل معالج منشئ المؤشر أختر أي عنوان ووصف ذي معنى للمؤشر الخاص بك، بعد ذلك تحقق من خانة الاختيار قائمة مراقبة عنوان URL. في هذه اللحظة يمكنك حفظ المؤشر، والا حاجة إلى مزيد من المعلومات، ومع ذلك، يمكنك إختيار تكوين باقي الخيارات المتاحة.



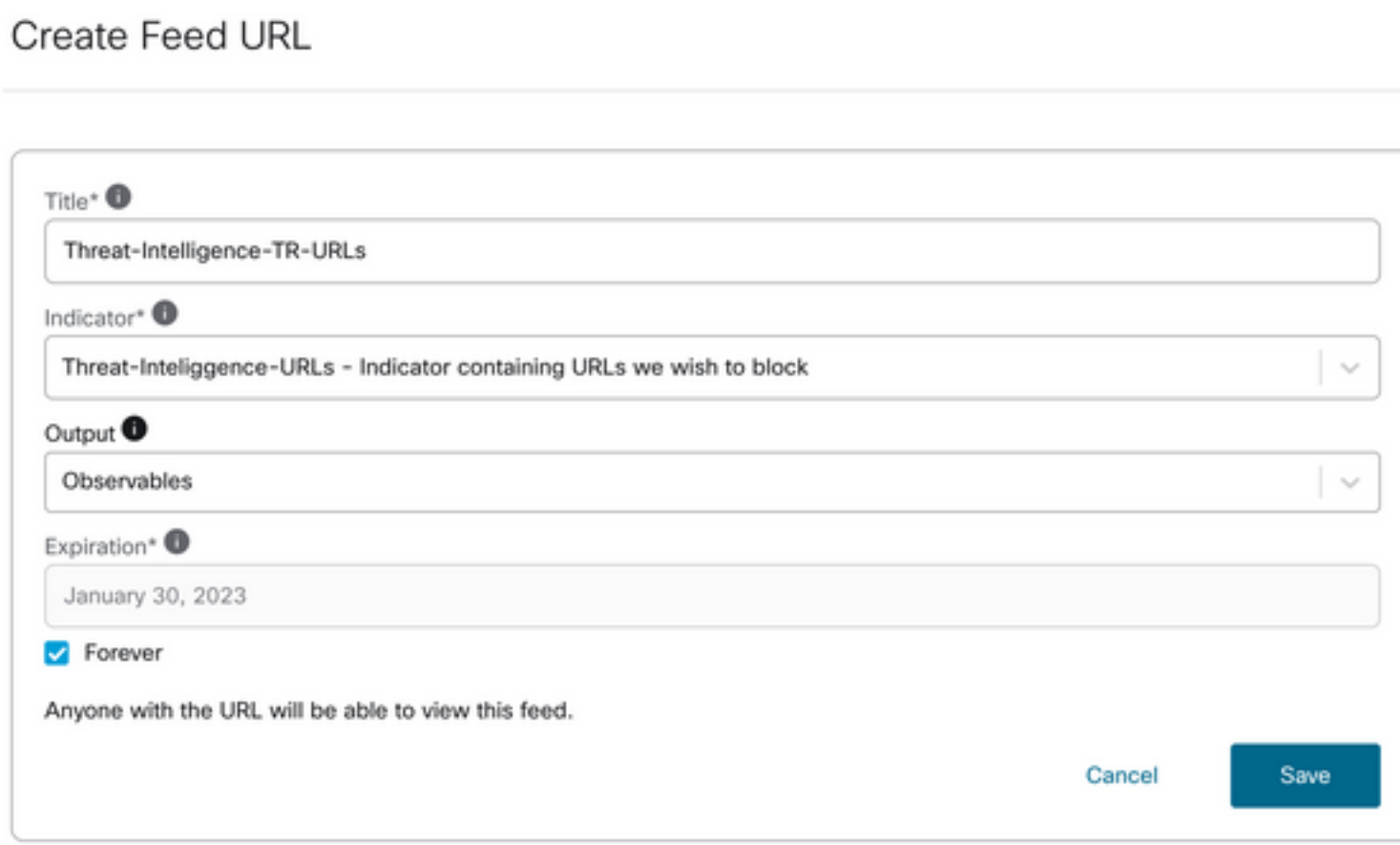
الخطوة 3 انتقل إلى علامة التبويب **التحقيق** ولصق أي ملف قابل للملاحظة ترغب في التحقيق فيه في مربع التحقيق. لأغراض توضيحية عنوان URL مزيف https://malicious-fake-domain.com تم إستخدامه لمثال التكوين هذا. انقر فوق **التحقيق** وانتظر انتهاء التحقيق. كما هو متوقع، فإن مصير URL غير معروف. استمر في النقر بزر الماوس الأيمن على السهم **لأسفل** لتوسيع القائمة السياقية وانقر **إنشاء حكم**.

الخطوة 4 انقر فوق **مؤشرات الارتباط** وحدد المؤشر من الخطوة 2. حدد المصير النهائي على أنه **ضار** واختر يوم انتهاء الصلاحية على النحو الذي تعتبره مناسبا. أخيرا انقر زر **إنشاء** . يجب أن يكون عنوان URL مرئيا الآن تحت **الذكاء > المؤشرات > عرض المؤشر الكامل**.

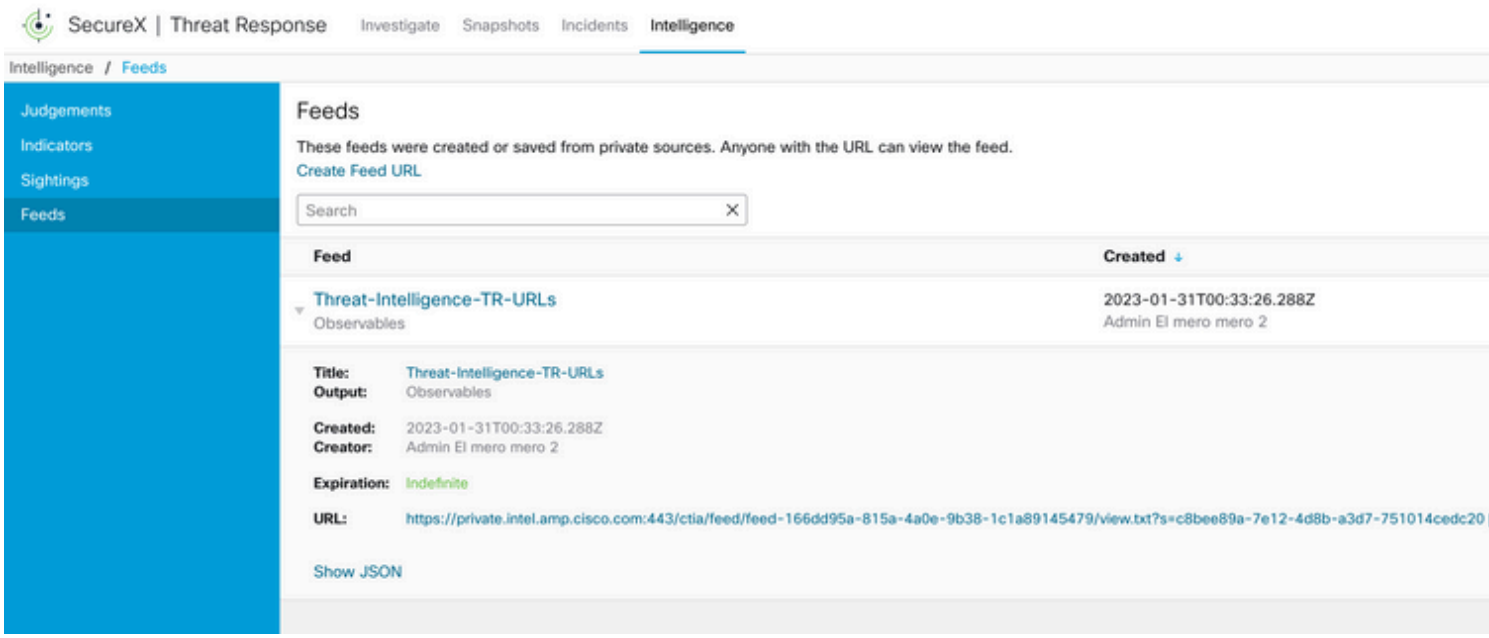




الخطوة 5 انتقل إلى **معلومات إستخبارية >موجز ويب** وانقر فوق **إنشاء عنوان URL لموجز الويب.** قم بتعبئة ملف **العنوان** ثم حدد المؤشر **الذي تم إنشاؤه** في الخطوة 2. تأكد من ترك قائمة المنسدل **الإخراج** كائنات **مرئية** وانقر فوق **حفظ.**



الخطوة 6 تأكد من إنشاء موجز الويب تحت **الذكاء > موجز الويب** ثم انقر للتوسيع على تفاصيل موجز الويب. انقر فوق **عنوان URL** لتظهر أن عناوين URL المتوقعة مدرجة في موجز الويب.



مدير إستخبارات تهديدات وحدة إدارة الاتصالات الفيدرالية (FMC) لاستهلاك موجز الاستجابة للتهديدات

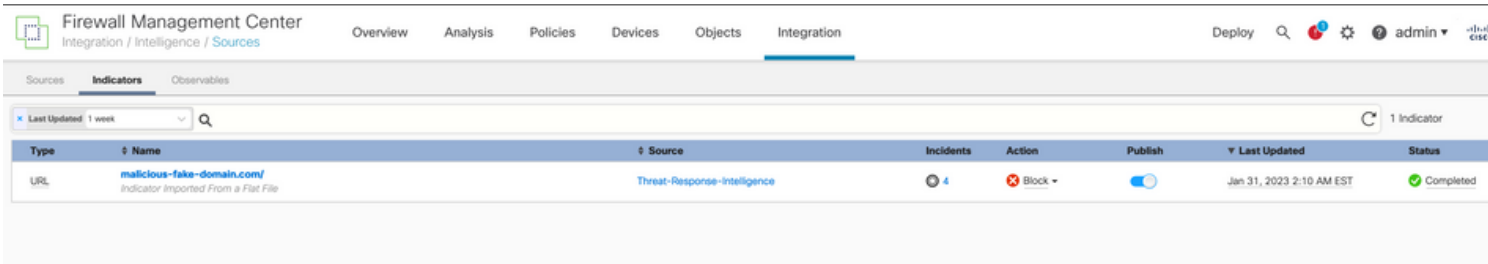
الخطوة 1 سجل الدخول إلى لوحة معلومات FMC وانتقل إلى **التكامل > الذكاء > المصادر**. **انقر فوق** تنبيهة **الإضافة** لإضافة مصدر جديد.

الخطوة 2 أنشيء المصدر الجديد مع هذا عملية إعداد:

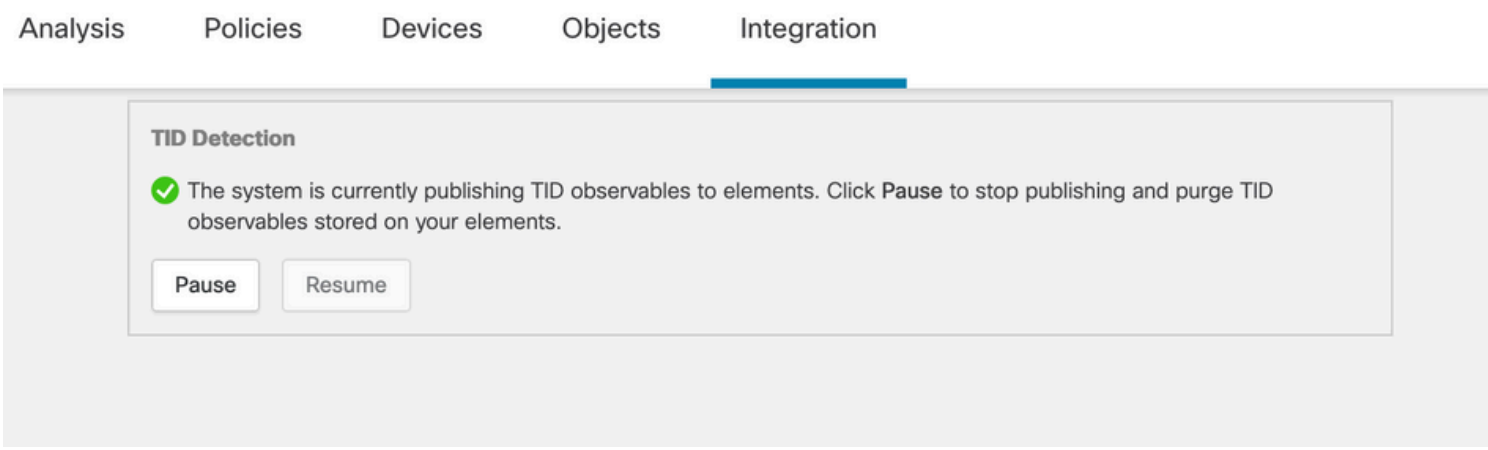
- التسليم > تحديد عنوان URL
- كتابة > تحديد ملف مسطح
- المحتوى > تحديد عنوان URL
- عنوان URL > لصق عنوان URL من القسم "إنشاء موجز إستجابة تهديدات SecureX" الخطوة 5.
- الاسم > إختيار أي اسم تراه مناسبا
- عملية > تحديد كتلة
- تحديث كل > تحديد 30 دقيقة (للتحديثات السريعة لموجز معلومات التهديد)

طقطقة **حفظ**.

الخطوة 3 تحت المؤشرات والنصوص القابلة للملاحظة التحقق من المجال مدرج:

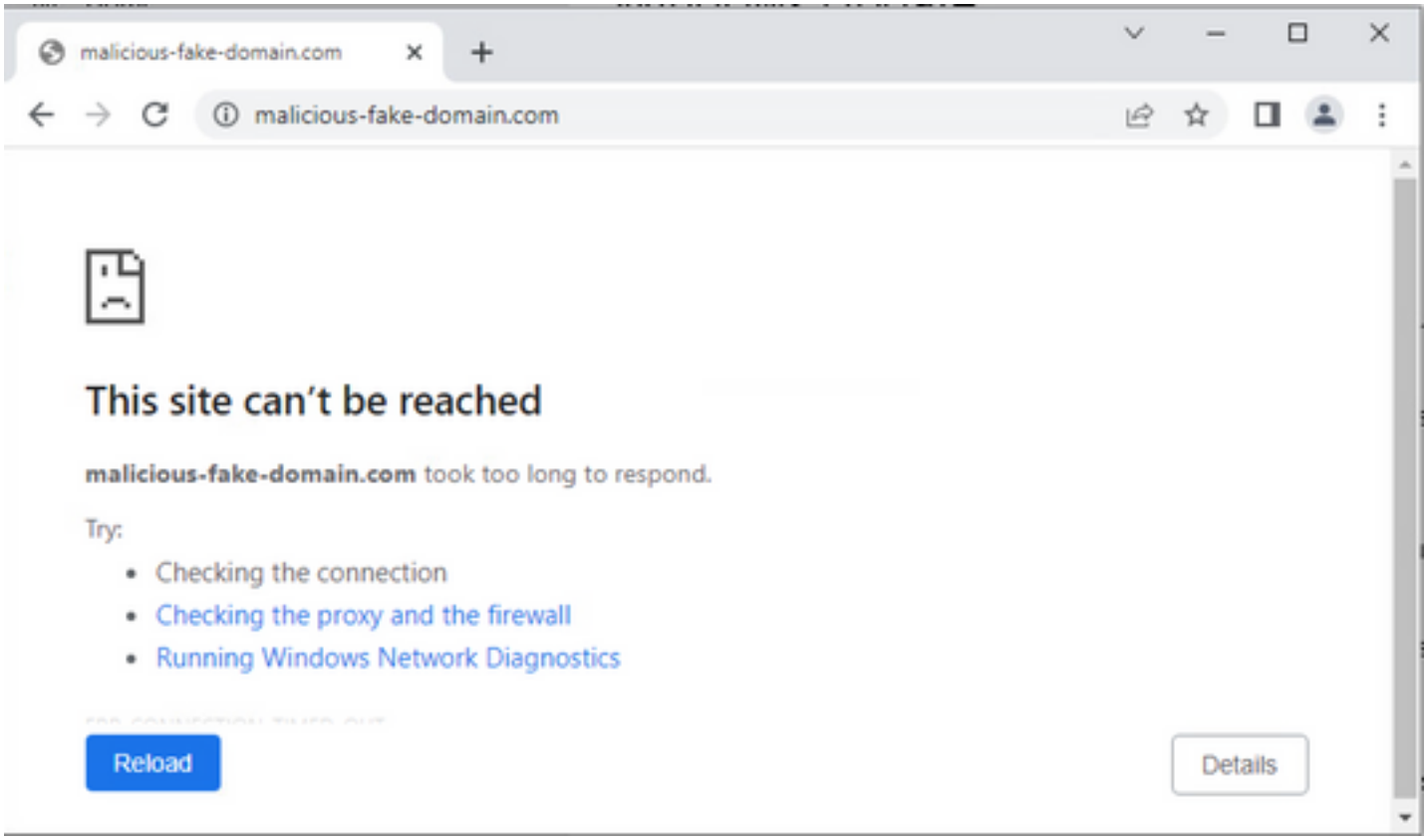


الخطوة 4 تأكد من أن مدير معلومات التهديد نشط وتحافظ على تحديث العناصر (أجهزة FTD). انتقل إلى **عمليات التكامل** > **الذكاء** > **العناصر**:

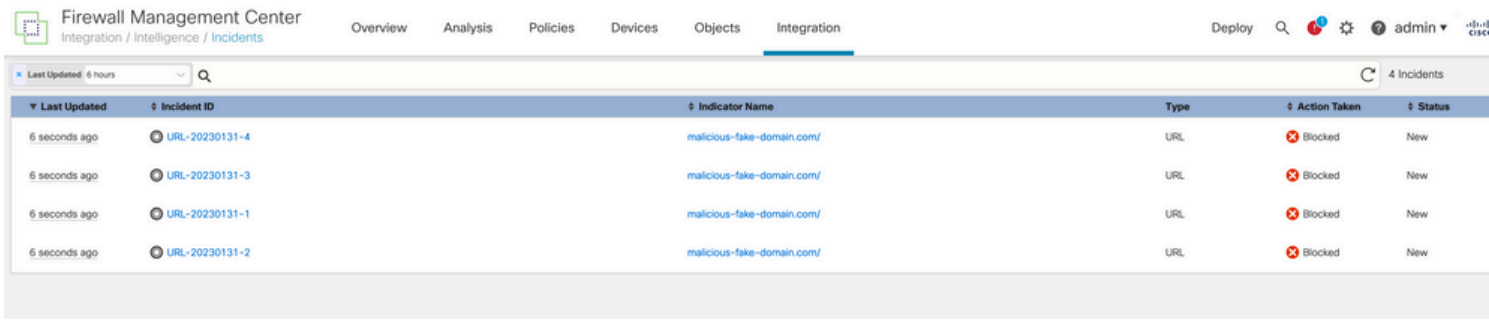


التحقق من الصحة

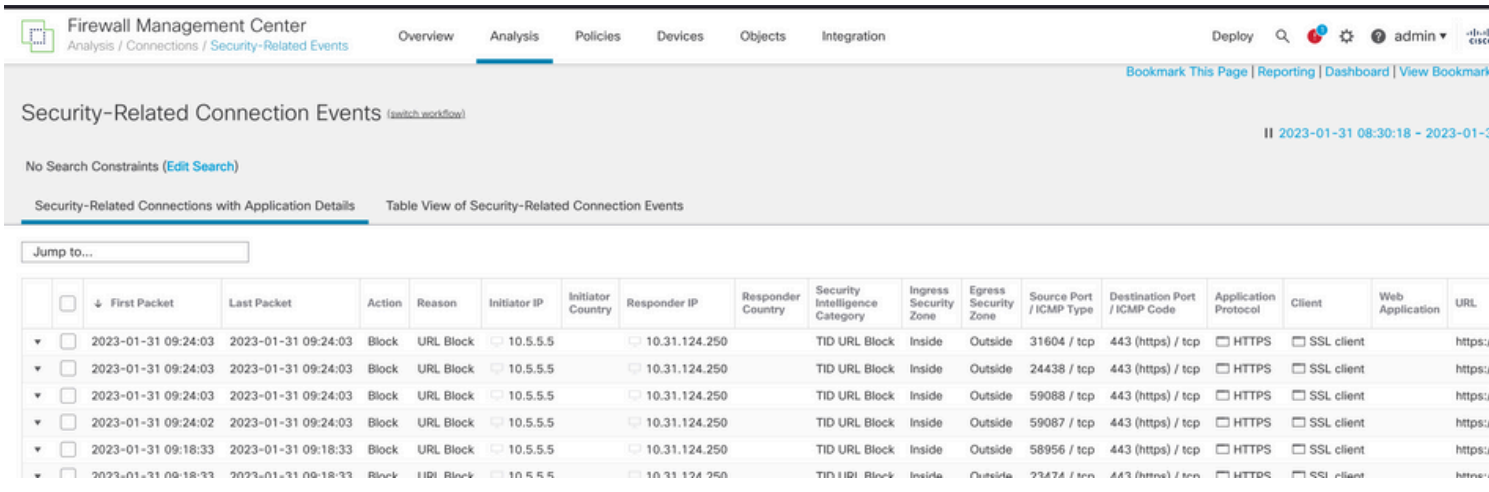
بعد اكتمال التكوين، تحاول نقطة النهاية الاتصال بعنوان URL https://malicious-fake-domain[.]com الذي تتم إستضافته على المنطقة الخارجية ولكن فشل الاتصالات كما هو متوقع.



للتحقق مما إذا كان فشل الاتصال ناجما عن انتقال موجز معلومات التهديد إلى عمليات التكامل > الذكاء > الحوادث. يجب سرد الأحداث المحظورة في هذه الصفحة.



يمكنك التحقق من أحداث الحظر هذه تحت Analysis (التحليل) > Connections > الأحداث المتعلقة بالأمان:



يتيح التقاط FTD LINA رؤية حركة المرور من نقطة النهاية إلى URL الضار عبر التحقق

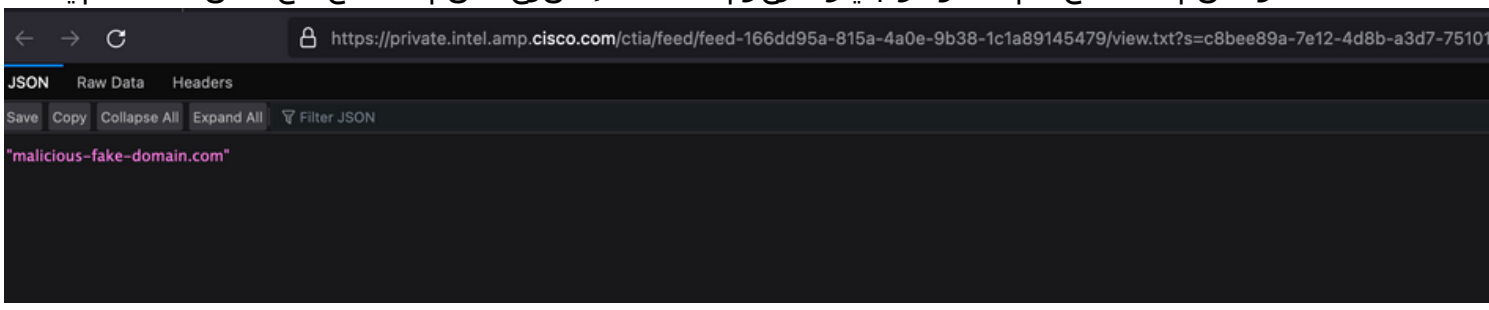
المتعدد. الرجاء، ملاحظة أنه تم التحقق من Snort Engine Phase 6 يعطي نتيجة إسقاط مرة أخرى، نظرًا لأن ميزة "معلومات التهديد" تستخدم محرك snort للكشف المتقدم عن حركة المرور. كن على علم، أن محرك snort يحتاج إلى السماح للزوجين الأولين من الحزم لتحليل وفهم طبيعة الاتصال لتشغيل الكشف بشكل صحيح. راجع قسم المعلومات ذات الصلة للحصول على مزيد من المعلومات حول التقاط FTD LINA.

```
7: 18:28:46.965449 0050.56b3.fd77 0050.56b3.de22 0x0800 Length: 571
10.5.5.5.63666 > 10.31.124.250.443: P [tcp sum ok] 2993282128:2993282645(517) ack 2622728404 win
1024 (DF) (ttl 128, id 2336)
Phase: 1
Type: CAPTURE
Subtype:
Result: ALLOW
Elapsed time: 1926 ns
Config:
Additional Information:
Forward Flow based lookup yields rule:
in id=0x14745cf3b800, priority=13, domain=capture, deny=false
hits=553, user_data=0x14745cf4b800, cs_id=0x0, l3_type=0x0
src mac=0000.0000.0000, mask=0000.0000.0000
dst mac=0000.0000.0000, mask=0000.0000.0000
input_ifc=Inside, output_ifc=any

Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Elapsed time: 1926 ns
Config:
Implicit Rule
Additional Information:
Forward Flow based lookup yields rule:
in id=0x14745c5c5c80, priority=1, domain=permit, deny=false
hits=7098895, user_data=0x0, cs_id=0x0, l3_type=0x8
src mac=0000.0000.0000, mask=0000.0000.0000
dst mac=0000.0000.0000, mask=0100.0000.0000
input_ifc=Inside, output_ifc=any

Phase: 3
Type: FLOW-LOOKUP
Subtype:
Result: ALLOW
Elapsed time: 3852 ns
Config:
Additional Information:
Found flow with id 67047, using existing flow
Module information for forward flow ...
snp_fp_inspect_ip_options
snp_fp_tcp_normalizer
snp_fp_tcp_proxy
snp_fp_snort
snp_fp_tcp_proxy
snp_fp_translate
snp_fp_tcp_normalizer
snp_fp_adjacency
snp_fp_fragment
snp_ifc_stat

Module information for reverse flow ...
snp_fp_inspect_ip_options
snp_fp_tcp_normalizer
```

```
snp_fp_translate
snp_fp_tcp_proxy
snp_fp_snort
snp_fp_tcp_proxy
snp_fp_tcp_normalizer
snp_fp_adjacency
snp_fp_fragment
snp_ifc_stat

Phase: 4
Type: EXTERNAL-INSPECT
Subtype:
Result: ALLOW
Elapsed time: 31244 ns
Config:
Additional Information:
Application: 'SNORT Inspect'

Phase: 5
Type: SNORT
Subtype: appid
Result: ALLOW
Elapsed time: 655704 ns
Config:
Additional Information:
service: HTTPS(1122), client: SSL client(1296), payload: (0), misc: (0)

Phase: 6
Type: SNORT
Subtype: SI-URL
Result: DROP
Elapsed time: 119238 ns
Config:
URL list id 1074790412
Additional Information:
Matched url malicious-fake-domain.com, action Block


Result:
input-interface: Inside(vrfid:0)
input-status: up
input-line-status: up
Action: drop
Time Taken: 813890 ns
Drop-reason: (si) Blocked or blacklisted by the SI preprocessor, Drop-location: frame
0x000056171ff3c0b0 flow (NA)/NA
```

استكشاف الأخطاء وإصلاحها

- للتأكد من أن إستجابة التهديد تبقي موجز الويب محدثا مع المعلومات الصحيحة التي يمكنك تصفحها على المستعرض إلى URL موجز الويب وترى الملاحظات المشتركة.



- لاستكشاف أخطاء برنامج Threat Intelligence Director التابع لوحدة التحكم الإدارية الخاصة وإصلاحها، يرجى التحقق من الارتباط على المعلومات ذات الصلة.

معلومات ذات صلة

- تكوين مدير معلومات تهديدات Cisco واستكشاف أخطائه وإصلاحها
- تكوين مدير معلومات تهديد جدار الحماية الآمن على FMC 7.3
- استخدام التقاط الدفاع عن تهديد FirePOWER وتتبع الحزم

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).